Symantec™ ApplicationHA agent for Internet Information Services Configuration Guide

Windows on Hyper-V

6.1

February 2014

Symantec

Symantec™ ApplicationHA agent for Internet Information Services Configuration Guide

Product_version: 6.1

Document_version: 6.1 Rev 0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/index.jsp

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/contact_techsupp_static.jsp

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

About Symantec Connect

Symantec Connect is the peer-to-peer technical community site for Symantec's enterprise customers. Participants can connect and share information with other product users, including creating forum posts, articles, videos, downloads, blogs and suggesting ideas, as well as interact with Symantec product teams and Technical Support. Content is rated by the community, and members receive reward points for their contributions.

http://www.symantec.com/connect/storage-management

Documentation

Your feedback on product documentation is important to us. Send suggestions for improvements and reports on errors or omissions. Include the title and document version (located on the second page), and chapter and section titles of the text on which you are reporting. Send feedback to:

doc_feedback@symantec.com

For information regarding the latest HOWTO articles, documentation updates, or to ask a question regarding product documentation, visit the Storage and Clustering Documentation forum on Symantec Connect.

https://www-secure.symantec.com/connect/storage-management/forums/storage-and-clustering-documentation

Contents

Chapter 1

Introducing ApplicationHA agents

This chapter includes the following topics:

About ApplicationHA agents

Agents are application-specific modules that plug into the ApplicationHA framework that manages the components of the configured applications.

The agents are installed when you install ApplicationHA. These agents start, stop, and monitor the components of the configured applications and report its state changes. If an application or its components fail, these agents restart the applications and its components on the virtual machine.

A virtual machine has one agent per component that monitors all the components of that type. For example, a single GenericService agent manages all services that are configured using the GenericService components. When the agent starts, it obtains the necessary configuration information from these components and then monitors the configured applications. The agents then periodically updates ApplicationHA with the component and application status.

Agents perform the following operations:

- Brings the components online

- Takes the components offline
- Monitors the components and reports the state changes

ApplicationHA agents are classified in the following categories:

- Infrastructure agents (bundled agents)
  Infrastructure agents are packaged (bundled) with the base software and include agents for mount points, generic services and processes. These agents are immediately available for use after you install ApplicationHA.
- Application agents
  Application agents are used to monitor third party applications such as Microsoft SQL Server, Microsoft Exchange and so on. These agents are packaged separately and are available in the form of an agent pack that gets installed when you install ApplicationHA.
  The agent pack is released on a quarterly basis. The agent pack includes support for new applications as well as fixes and enhancements to existing agents. You can install the agent pack on an existing ApplicationHA installation.
  Refer to the Symantec Operations Readiness Tools (SORT) Website for information on the latest agent pack availability:
  https://sort.symantec.com

This document describes the ApplicationHA bundled agents along with their resource type definitions, attribute definitions, and sample configurations.

About intelligent monitoring framework

ApplicationHA provides Intelligent Monitoring Framework (IMF) to determine the status of the configured application and its components. IMF employs an event-based monitoring framework that is implemented using custom as well as native operating system-based notification mechanisms.

IMF provides instantaneous state change notifications. ApplicationHA agents detect this state change and then trigger the necessary actions.

IMF provides the following key benefits:

- Instantaneous notification
  Faster fault detection resulting in faster fail over and thus less application down time.
- Ability to monitor large number of components
  With reduced CPU consumption, IMF effectively monitors a large number of components.
- Reduction in system resource utilization

Reduced CPU utilization by ApplicationHA agent processes when number of components being monitored is high. This provides significant performance benefits in terms of system resource utilization.

About the agent functions and attributes

Every agent has a collection of attributes and performs a definite set of functions.

Attributes are the set of variables whose values configures the corresponding application component to function in a specific way. By modifying attribute values you can change the way in which ApplicationHA agent manages the component.

For example, the IP agent monitors an IP address. The specific address to be monitored is identified by the attribute "Address" whose value is the specific IP address.

Depending on the category to which an agent belongs, an agent performs either or all of the following functions:

Online	Brings the configured component online
Offline	Takes the configured component offline
Monitor	Verifies if the configured component is online

As part of the Monitor function, an agent reports the following states:

ONLINE	Indicates that the configured component is online
OFFLINE	Indicates that the configured component/application has faulted
UNKNOWN	Indicates that the agent encountered errors while monitoring the configured component

About the ApplicationHA agent for Internet Information Services

The ApplicationHA for Hyper-V agent for IIS provides monitoring support for sites configured using Microsoft Internet Information Services (IIS).

The agent monitors the Websites and the associated application pools configured on a virtual machine. The agent brings IIS sites online, monitors their status, and takes them offline.

The agent provides the following ways of monitoring application pools associated with IIS Web sites:

- One IIS resource configures a Web site and sets monitoring options for application pools associated with the site
- One IIS resource configures a Web site; other resources configure individual application pools

Agent functions

Online	Starts the configured site or application pool
Offline	Stops the configured site or application pool
Monitor	Verifies the configured site and confirms if the application pool is running

Agent state definitions

ONLINE	Indicates that the configured site or application pool is available
OFFLINE	Indicates that the configured site or application pool is not available
UNKNOWN	Indicates that the agent cannot determine the status of the resource

Resource type definition

```
type IIS (
static i18nstr ArgList[] = {SiteType, SiteName,
"IPResName:Address", PortNumber, AppPoolMon, DetailMonitor,
DetailMonitorInterval }
str SiteType
i18nstr SiteName
int PortNumber
str AppPoolMon = NONE
boolean DetailMonitor = 0
int DetailMonitorInterval = 5
str IPResName
)
```

Agent attributes

Table 1-1describes the required attributes for the ApplicationHA agent for IIS.

Note: To configure the agent to monitor an application pool, configure the SiteType and SiteName attributes only. The agent ignores other attributes when it is configured to monitor an application pool.

Table 1-1 Required attributes for the ApplicationHA agent for IIS

Required attributes	Description
SiteType	Defines whether the resource is configured to monitor an IIS site or an application pool. If the resource is configured to monitor an application pool, set the attribute to APPPOOL. If the resource is configured to monitor an IIS site, set this attribute to the name of the IIS service associated with the site. The attribute can take any of the following values: ■ W3SVC ■ MSFTPSVC ■ SMTPSVC ■ NNTPSVC Type and dimension: string-scalar
SiteName	The name of the IIS site, or the application pool to be monitored by the agent. The value of this attribute depends on the value of the SiteType attribute. The SiteName attribute can take the following values: ■ The name of a site, if SiteType is W3SVC or MSFTPSVC ■ The name of a virtual server, if SiteType is SMTPSVC or NNTPSVC ■ The name of an application pool, if SiteType is APPPOOL Type and dimension: string-scalar
IPResName	The name of the IP resource configured for the IP to which the site is bound. Type and dimension: string-scalar
PortNumber	This attribute is not applicable for Microsoft Internet Information Services (IIS).

Table 1-2describes the optional attributes for the ApplicationHA agent for IIS

Table 1-2 Optional attributes for ApplicationHA agent for IIS

Optional attribute	Description
AppPoolMon	Defines the monitoring modes for the application pool associated with the Web site being monitored. Configure this attribute only if SiteType isW3SVCand IIS is configured to run in the Worker Process Isolation mode. The attribute can take one of the following values: ■ NONE: Indicates that the agent will not monitor the application pool associated with the Web site. ■ DEFAULT or ALL: Indicates that the agent will monitor the application pool associated with the Web site. If this attribute is set, the agent starts, stops, and monitors the application pool associated with the Web site. If the application pool is stopped externally, the agent fails over the service group. Type and dimension: integer-scala
DetailMonitor	A flag that defines whether the agent monitors the site in detail. The value 1 indicates the agent will monitor each site in detail by attempting an actual socket connection to the port. Default is 0, which means that detail monitoring is disabled by default. Type and dimension: boolean-scalar
DetailMonitorInterval	The number of monitor cycles after which the agent attempts detail monitoring. For example, the value 5 indicates that the agent will monitor the resource in detail after every 5 monitor cycles. This attribute is ignored if DetailMonitor is set to 0. Default is 5. Type and dimension: integer-scalar

How ApplicationHA agents monitor Internet Information Services

The ApplicationHA agent for Internet Information Services monitors the configured resources, determines the status of these resources, brings them online, and takes them offline. The agent detects an application failure if the configured IIS Web sites

or application pools become unavailable. The agent then tries to start the Web sites for a configurable number of attempts. If the configured Web sites do not start, the agent considers this as an application failure and reports the "Application critical state" to the Hyper-V host.

Depending on the configuration, the Hyper-V host then restarts the virtual machine. After the virtual machine restarts, the agent starts the configured Web sites and the associated application pools and brings the configured resources online on the system.

Chapter 2

Configuring application monitoring

This chapter includes the following topics:

Considerations for configuring application monitoring

Symantec ApplicationHA provides an interface, Symantec ApplicationHA Health View, to configure and administer application monitoring.

A shortcut to access the Health View is created on the system's desktop after you install ApplicationHA. The Health View is Web-based and can be accessed using any of the available browser.

You can also access the Health View directly from a browser window using the following URL:

https://*VMNameorIP*:5634/vcs/admin/application_health.html?priv=ADMIN

Consider the following before you configure application monitoring:

- You can configure application monitoring on a virtual machine using the Symantec ApplicationHA Configuration Wizard. The wizard is launched when you click **Configure Application Monitoring** on the Symantec ApplicationHA Health View.
- You can use the wizard to configure monitoring for only one application per virtual machine.
  To configure application monitoring on the same virtual machine, for any additional applications, you must use the VCS commands.

To configure another application using the wizard, you must first unconfigure the existing application monitoring configuration.

- The wizard runs in a logged-on user context. You must thus ensure that the logged-on user has administrative privileges on the virtual machine where you want to configure application monitoring.
- If you have configured a firewall, ensure that your firewall settings allow access to ports used by Symantec ApplicationHA installer, wizard, and services.
  For information about the ports used, refer to the *Symantec ApplicationHA Deployment Guide*.
- If the application data is stored on nested mount points, then it is required to set the dependency between these mount points. This enables ApplicationHA to monitor all the nested mount points.
  To define the dependency between the nested mount points, you must set the value for MountDependsOn attribute of the MountMonitor agent. The value of this attribute must be specified as a key-value pair.
  Where,
  Key= mount path
  Value= volume name
- After configuring IIS Web sites for monitoring, if you create another site or application pool, then these new components are not monitored as part of the existing configuration.
  In this case, you can either use the VCS commands to add the components to the configuration or unconfigure the existing configuration and then run the wizard again to configure all the components.

Note: When you configure or unconfigure application monitoring, it does not affect the state of the application. The application runs unaffected on the virtual machine.

- IIS lets you create sites with duplicate bindings but only one site can run at a time. After configuring an IIS site for monitoring, if you create another Web site with the same IP:Port:HostHeader binding, it may potentially affect the existing configuration.
  To understand how this affects the monitoring configuration, consider the following example.
  Configure and start monitoring a site with Symantec ApplicationHA. Then, from IIS add another site with the same bindings as the configured site. IIS will let you create the site but you will not be able to start it.
  From the ApplicationHA view, stop the site that is configured for monitoring. Then from IIS start the other site that has duplicate bindings.

Now, if you try to start the configured site from the ApplicationHA view, IIS will not allow the site to run as another site with the same binding is already running on the system. This may lead to a situation where Symantec ApplicationHA is unable to start the configured site on the system and may report the "Applications Critical" status to the Hyper-V host. If the virtual machine is restarted, Symantec ApplicationHA will still not be able to start the configured IIS site on the virtual machine as there are two sites having the same bindings. As a result the monitoring configuration will not serve its purpose.

You must therefore ensure that virtual machines where you configure IIS monitoring host sites with unique bindings.

- For IIS 7.0, you must install the following role services:
  - IIS 6 Metabase Compatibility
  - IIS 6 WMI Compatibility or the IIS Management Scripts and Tools These options are available under Management Tools on the Role Services page of the Add Roles Wizard.

    If IIS 6 Metabase Compatibility role is installed, the WMI 6 Provider is used. If IIS Management Scripts and Tools role is installed, the WMI 7 Provider is used. If both the roles are installed, the WMI 7 Provider is used.
- Ensure that you have installed IIS and configured the sites and application pools that you want to monitor on the virtual machine.
- Ensure that the sites have unique IP:Port bindings, host header names, and site names.

Configuring application monitoring

Perform the following steps to configure monitoring for Internet Information Services on a virtual machine using the Symantec ApplicationHA Configuration Wizard.

Note: You can configure monitoring for multiple services and processes in a single wizard workflow. However, you cannot configure multiple applications simultaneously. To configure another application, run the wizard again.

To configure application monitoring for Internet Information Services

1. Launch the Symantec ApplicationHA Health View, using the shortcut created or in a browser, using the following URL:

   https://*VMNameorIP*:5634/vcs/admin/ application_health.html?priv=ADMIN

2. Click **Configure Application Monitoring** to launch the Symantec ApplicationHA Configuration Wizard.

3. Review the information on the Welcome panel and then click **Next**.

4. On the Application Selection panel, click **Internet Information Services** in the Supported Applications list.

5. On the IIS Site Selection panel, select the IIS sites and the associated applications pools that you want to monitor and then click **Configure**.

   For each selected site you must select the application pool monitoring options from the corresponding drop-down list.

   The following options are available:

   - Default: Starts and monitors the root application pool associated with the site.
   - All: Starts all the application pools associated with the selected site and monitors the root application pool.
   - None: Does not monitor the application pools associated with the selected site.

6. On the ApplicationHA Configuration panel, the wizard performs the application monitoring configuration tasks, creates the required resources, and enables the application heartbeat that communicates with Hyper-V host.

   The panel displays the status of each task. After all the tasks are complete, click **Next**.

   If the configuration tasks fail, click **View Logs** to check the details of the failure. Rectify the cause of the failure and run the wizard again to configure the application monitoring.

7. On the Finish panel, click **Finish** to complete the wizard.

   This completes the application monitoring configuration.

   Use the ApplicationHA Health View to monitor the application status and control application monitoring.

   For more details refer to the *Symantec ApplicationHA Deployment Guide*.

Index